CLAIMS

1. A device for performing bidirectional control in digital bidirectional communication, comprising:

an interface block for converting a format of input downstream data to generate downward data;

a CPU which receives the downward data and realizes a MAC (Media Access Control) function; and

a TEK process block for receiving TEK (Traffic Encryption Key) process data obtained from the downward data, analyzing a data structure of the TEK process data, and performing decryption processing based on a result of the analysis.

2. The device of claim 1, wherein the TEK process block includes:

a structure analysis block for analyzing an MPEG structure included in the received TEK process data and a MAC (Media Access Control) structure buried in the MPEG structure to output MAC state information data that represents a state and meaning of MAC data having the MAC structure;

a decryption block for identifying encrypted part of the TEK process data by referring to the MAC state information data, decrypting the encrypted part using TEK data for cryptanalysis, and integrating a result of the decryption with unencrypted part of the TEK process data.

3. The device of claim 2, wherein the structure analysis block includes:

an MPEG header analysis block for analyzing an MPEG header of the MPEG structure included in the TEK process data to output a MAC data position signal which indicates a position of the MAC data and a MAC data head position signal which indicates

a position of a leading byte of a MAC frame;

a MAC header analysis block for receiving the MAC data position signal and the MAC data head position signal and determining a state information for fields included in a MAC header of the MAC structure except for an extension header and a MACMM (MAC Management Message) header, wherein the MAC header analysis block outputs extension header position information data which indicates a position of the extension header when the TEK process data includes the extension header, and the MAC header analysis block outputs MACMM header position information data which indicates a position of the MACMM header when the TEK process data includes the MACMM header;

an extension header analysis block for receiving the extension header position information data and checking fields of the extension header to output extension header state information data which represents state information of the extension header; and

a MACMM header analysis block for receiving the MACMM header position information data and checking fields of the MACMM header to output MACMM header state information data which represents state information of the MACMM header,

wherein the MAC header analysis block receives the extension header state information data and the MACMM header state information data and generates the MAC state information data based on state information of the fields included in the MAC header except for the extension header and MACMM header, the state information of the extension header which is represented by the extension header state information data, and the state information of the MACMM header which is represented by the MACMM header state information data.

4. The device of claim 3, wherein the MPEG header analysis block checks a field of an MPEG header to detect a position of the MAC data and a position of a leading byte of the

MAC frame and output the MAC data position signal and the MAC data head position signal.

5. The device of claim 3, wherein the MAC header analysis block performs a HCS check to detect an error in the MAC header.

6. The device of claim 3, wherein:

the MAC header analysis block performs a check on a field which indicates a MAC data length in the MAC header; and

the check is realized by referring to the MAC data head position signal to count a data length of the MAC frame and determine whether or not the MAC frame length is equal to the sum of the value of the field and a predetermined data length.

7. The device of claim 3, wherein:

the MAC header analysis block performs a MAC frame length check and an extension header length check in addition to the HCS check, thereby detecting an error in the MAC header; and

if check results of the MAC frame length check and the extension header length check are no error, the MAC header analysis block invalidates a check result of the HCS check.

8. The device of claim 3, wherein:

the extension header analysis block refers to the extension header position information data to check a field of the extension header and determine the data length and type of the extension header; and

if the value of the field of the extension header is invalid, the extension header

analysis block determines that there is an error in the extension header and outputs the determination result as the extension header state information data.

9. The device of claim 3, wherein:

the MACMM header analysis block refers to the MACMM header position information data to check a field of the MACMM header and determine the data length and type of the MACMM header; and

if the value of the field of the MACMM header is invalid, the MACMM header analysis block determines that there is an error in the MACMM header and outputs the determination result as the MACMM header state information data.

10. The device of claim 2, wherein the decryption block performs the steps of:

referring to the MAC state information data to identify encrypted part and unencrypted part of the TEK process data;

extracting from the TEK process data TEK collation data for selecting TEK data;

referring to the extracted TEK collation data to select TEK data used for decryption from a plurality of items of pre-stored TEK data;

converting the encrypted part so as to have a bit width equal to a unit of decryption processing and decrypting the converted encrypted part using the selected TEK data; and

integrating the decrypted data and the unencrypted part.

11. A method for performing bidirectional control in digital bidirectional communication, comprising:

the step of converting a format of downstream data to generate downward data;

the step of receiving the downward data to realize a MAC (Media Access Control) function by a CPU; and

a TEK process step of receiving TEK (Traffic Encryption Key) process data obtained from the downward data at a TEK process block to analyze a data structure of the TEK process data and performs decryption processing based on a result of the analysis.

12. The method of claim 11, wherein the TEK process step includes:

a structure analysis step of analyzing an MPEG structure included in the TEK process data and a MAC (Media Access Control) structure buried in the MPEG structure to generate MAC state information data which represents a state and meaning of MAC data having the MAC structure; and

a decryption step of referring to the MAC state information data to identify encrypted part of the TEK process data, decrypting the encrypted part using TEK data for cryptanalysis, and integrating a result of the decryption with unencrypted part of the TEK process data.

13. The method of claim 12, wherein the structure analysis step includes:

an MPEG header analysis step of analyzing an MPEG header of the MPEG structure of the TEK process data to generate a MAC data position signal which indicates a position of the MAC data and a MAC data head position signal which indicates a position of a leading byte of a MAC frame;

a MAC header analysis step of determining a state information for fields included in a MAC header of the MAC structure except for an extension header and a MACMM (MAC Management Message) header using the MAC data position signal and the MAC data head position signal, wherein extension header position information data which indicates a position of the extension header is generated when the TEK process data

includes the extension header, and MACMM header position information data which indicates a position of the MACMM header is generated when the TEK process data includes the MACMM header;

an extension header analysis step of receiving the extension header position information data and checking fields of the extension header to output extension header state information data which represents state information of the extension header; and

a MACMM header analysis step of receiving the MACMM header position information data and checking fields of the MACMM header to output MACMM header state information data which represents state information of the MACMM header,

wherein the MAC state information data is generated based on state information of the fields included in the MAC header except for the extension header and the MACMM header, which has been determined at the MAC header analysis step, the state information of the extension header which is represented by the extension header state information data, and the state information of the MACMM header which is represented by the MACMM header state information data.